Relay attacks on HF RFID and NFC communications and defense against them*

Tamás Varga[a], **Róbert Schulcz**[b]

[a]BME Mobil Innovációs Központ
tvarga@mik.bme.hu

[b]BME Mobil Innovációs Központ
rschulcz@mik.bme.hu

Abstract

Relay attacks are attacks on systems' security involving a malicious third party interrupting communication between legitimate parties A and B. During a relay attack the malicious third party forwards messages between parties A and B without changing any of the messages thus relay attack can be interpreted as a special case of man-in-the-middle attacks. Its purpose is often eavesdropping on communication links but relay attack is also capable to change the chronology of events and extending the range of the communication link. The relay attack against RFID or NFC communication links is often carried out to impersonate a device at a distant location. In our work our goal is to discuss the general properties of attacks and specifically the relay attacks on RFID and NFC systems and to enumerate the relay attacks on RFID and NFC devices discussed in papers. Our work also contains thoughts of feasible defense techniques against the relay attacks.

References

[1] G. Hancke, Design of a secure distance-bounding channel for RFID.

[2] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, Classification of RFID Attacks.

[3] L. Francis, G. Hancke, K. Mayes and K. Markantonakis, „Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones".

[4] G. Hancke, „A Practical Relay Attack on ISO 14443 Proximity Cards," (2005).

*This article was financed by the project TÁMOP-4.2.2.C-11/1/KONV-2012-0014 FutureRFID - Az RFID/NFC technológia továbbfejlesztési lehetőségei az "Internet of Things" koncepció mentén.

[5] Z. Kfir and A. Wool, „Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," Tel Aviv University.

[6] Y. Oren and A. Wool, „Relay Attacks on RFID-Based Electronic Voting Systems".

[7] M. Roland, „Applying Relay Attacks to Google Wallet," Zürich, (2013).

[8] P.-H. Thevenon, O. Savry, S. Tedjini and R. Malherbi-Martins, „Attacks on the HF Physical Layer of Contactless and RFID Systems".

[9] M. Roland, „Relay Attacks on Secure Element-enabled Mobile Devices Virtual Pickpocketing Revisited".

[10] M. Hlavac and T. Rosa, „A Note on the Relay Attacks on e-passports".

[11] M. Weiss, „Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobil Equipment," Der technischen Universität München, (2010).

[12] A. Czeskis, K. Koscher, J. R. Smith and T. Kohno, „RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications".